



## MIDLOTHIAN INDEPENDENT SCHOOL DISTRICT

# ACCEPTABLE USE PROCEDURES

Midlothian ISD offers Internet access for students and teachers. The use of the Internet is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges. This document contains the Acceptable Use Procedure for using the MISD Electronic Communication System. The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.

### >CONSENT REQUIREMENTS

No original work created by any District student or employee will be posted on a webpage under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work.

No personally identifiable information about a District student will be posted on a webpage under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy.

### >FILTERING

The Superintendent will appoint a committee, to be chaired by the technology coordinator, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors, in compliance with the Children's Internet Protection Act (CIPA) {Pub. L. No. 106-554 and 47 USC 254(h)}. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

### >REQUESTS TO DISABLE FILTER

The committee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The committee will make recommendation to the Superintendent regarding approval or disapproval of disabling the filter for the requested use.

### >SYSTEM ACCESS

1. Students granted access to the District's system must complete any applicable District network training.
2. As appropriate and with the written approval of the immediate supervisor and completion of District network training, District employees will be granted access to the District's system.
3. Teachers are required to have a First Class account and they are ultimately responsible for use of the account.
4. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.
5. All users will be required to sign a user agreement annually for issuance or renewal of an account.

## >INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines: This includes arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of persons, etc.
3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
6. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
7. System users should refer to the Midlothian ISD Webpage Guidelines when sharing student work online. K-5th grade students' work and photo may be posted and identified using first name and last initial only. 6th - 12th grade student work and photographs may be posted with full name identification. No other personal information about a student is allowed, such as e-mail address, home number, or home address.
8. System users should refer to the Midlothian ISD Guidelines for Educators Using Social Networking Sites for district recommendations.
9. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any request for such a meeting.
10. System users must purge electronic mail in accordance with established retention guidelines.
11. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
12. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
13. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.
14. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
15. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
16. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
17. System users may not waste District resources related to the electronic communications system: This includes spamming and participation in discussion group mail lists that are not relevant to education or career development.
18. System users may not gain unauthorized access to resources or information.
19. System users may not use the System for political lobbying. It may be used to communicate with elected representatives to express opinions on political issues.
20. System users may not use the system for commercial business.
21. Secondary system users may bring their own devices from home including readers, tablets, netbooks, and laptops for use in an instructional setting. This does not include cell phones.

## >VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and

administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

#### >FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

#### >INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

#### >DISTRICT WEBSITE

The District will maintain a District website for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District website must be directed to the designated Webmaster. The Technology Coordinator and the District Webmaster will establish guidelines for the development and format of webpages controlled by the District.

No personally identifiable information regarding a student will be published on a website controlled by the District without written permission from the student's parent on the Family Education Rights and Privacy Act (FERPA) form.

No commercial advertising will be permitted on a website controlled by the District without prior approval of the Superintendent.

#### >SCHOOL OR CLASS WEBPAGES

Campuses may create school websites using district resources and may link to appropriate campus social media accounts, subject to approval from the district's Webmaster. The campus principal will designate the staff member responsible for managing the campus' webpage under the supervision of the district's Webmaster. Teachers will be responsible for compliance with District rules in maintaining their class webpages.

#### >STUDENT WEBPAGES

With the approval of the District Webmaster, students may establish individual webpages linked to a campus or District website; however, all material presented on a student's webpage must be related to the student's

educational activities. Student webpages must include the following notice: "This is a student webpage. Opinions expressed on this page shall not be attributed to the District." Any links from a student's webpage to sites outside the District's computer system must receive approval from the District Webmaster or campus website designee.

#### >ONLINE COMMUNICATION TOOLS

Teachers, administrators, librarians, or counselors may create online communication tools for use in class activities or to provide a resource for other teachers or staff members in the District. Teachers will be responsible for maintaining their class or educational online communication tools.

#### >EXTRA- CURRICULAR ORGANIZATION WEBPAGES

With the approval of the campus principal or designee, extracurricular organizations may establish webpages and/or social media accounts. All material presented on these sites must relate specifically to organization activities and include information relevant to the club. The sponsor of the organization will be responsible for complying with District rules for maintaining the webpage and/or social media accounts. Extracurricular organizations must include the following notice: "This is a student extracurricular organization webpage or social media account. Opinions expressed on this page shall not be attributed to the District."

#### >PERSONAL WEBPAGES

District employees, Trustees, and members of the public will not be permitted to publish personal webpages using District resources.

#### >NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.

Using the network in such a way that would disrupt the use of the network by other users is prohibited.

#### >TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District Coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

#### >DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

#### >COPYRIGHT COMPLIANCE

The use of District technology in violation of any law, including copyright law, is prohibited. Copyrighted or licensed software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright or license. Only the copyright or license owner, or an individual the owner specifically authorizes, may upload copyrighted or licensed material to the system.

No person will be allowed to use the District's technology to post, publicize, or duplicate information in violation of copyright law. The Technology Coordinator will use all reasonable measures to prevent the use of District technology in violation of the law.

#### >COMPLAINTS REGARDING COPYRIGHT COMPLIANCE

If a copyright or license owner reasonably believes that the District's technology has been used to infringe upon a copyright or license, the owner is encouraged to notify the District.

The District designates the following employee to receive any complaints that copyrighted material is improperly contained in the District network:

Name: Mr. Kirk Paschall

Position: Executive Director of Technology

Address: 100 Walter Stephenson Road, Midlothian, TX 76065

Telephone: 972-775-8296

E-mail: [kirk\\_paschall@midlothian-isd.net](mailto:kirk_paschall@midlothian-isd.net)